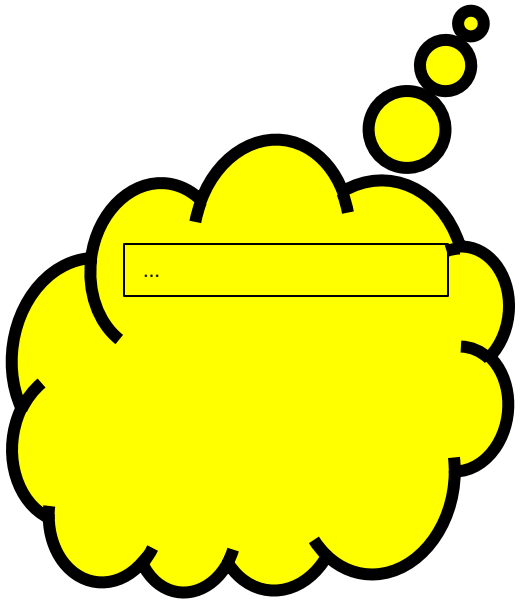
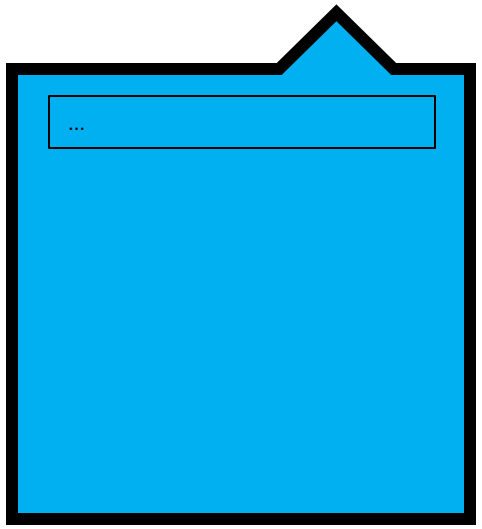
USCITE DI SICUREZZA

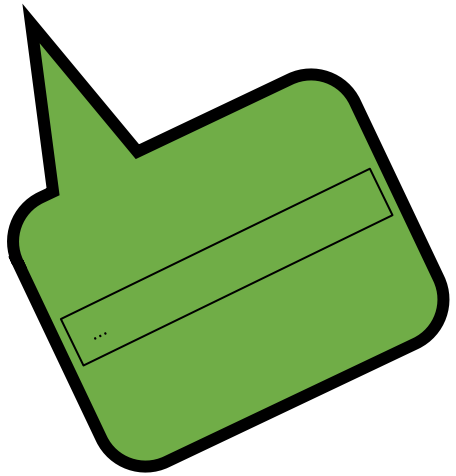
INCONTRO UNO

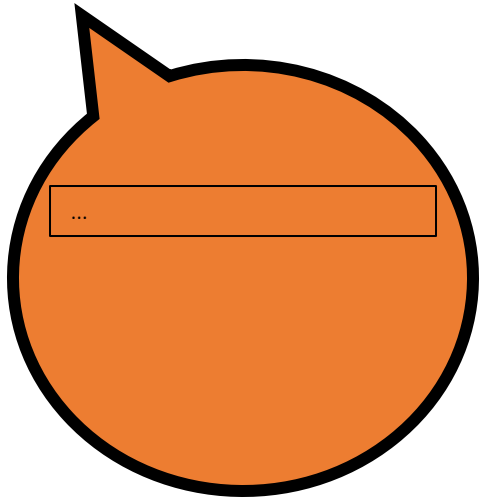
CYBER SECURITY E PASSWORD

COS'E', SECONDO VOI, LA CYBER SICUREZZA?









VIRUS E ALTRI DEMONI

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/alk335k1i2p8

Cos'è la cyber security o Sicurezza informatica?

La *cybersecurity* è l'insieme di tecnologie e procedure in grado di **proteggere i sistemi informatici**, in particolare la loro integrità.

Due caratteristiche spiegano al meglio il concetto di cyber sicurezza:

- **Safety**: una serie di azioni in grado di eliminare la produzione di danni all'interno del sistema stesso;
- **Reliability**: la prevenzione nei confronti di eventi che possono causare danni di diversa gravità al sistema.

In linea generale, la **sicurezza di un software** dipende dalla possibilità che vi è di danneggiarlo in maniera irreparabile, in una scala che va da «**nessun effetto**» fino a «**rischio catastrofico**».

La sicurezza informatica serve, quindi, a monitorare le vulnerabilità presenti all'interno del sistema informatico, passando per l'attuazione di servizi di prevenzione e di risposte alle minacce esterne.

SAFE SURFING

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/aloy83zzaahj

Cosa significa veramente «occuparsi di sicurezza informatica?»

La sicurezza informatica è una vasta area professionale che coinvolge diverse specializzazioni.
Ecco alcune delle principali professioni legate alla sicurezza informatica:

- Esperto di sicurezza informatica: sviluppa strategie per proteggere i sistemi informatici dalle minacce esterne e interne. Svolge un ruolo fondamentale nel prevenire e rispondere alle violazioni della sicurezza.
- Analista di sicurezza informatica: si occupa di analizzare i sistemi informatici e di individuare le vulnerabilità. Il loro lavoro consiste nel testare e monitorare i sistemi per proteggerli da eventuali minacce.
- Incident Response Analyst: risponde ai casi di violazione della sicurezza e di ripristino della sicurezza dei sistemi informatici. Svolge anche un ruolo fondamentale nell'identificare le cause della violazione e nel proporre soluzioni per prevenirne di nuove.
- Architetto di sicurezza informatica: progetta e implementa soluzioni di sicurezza informatica per i sistemi informatici. Il loro lavoro consiste nel garantire che i sistemi siano costruiti in modo sicuro e che le informazioni siano protette dalle minacce esterne e interne.
- Ethical Hacker: conosciuto anche come *hacker etico*, si occupa di testare i sistemi informatici per identificare le vulnerabilità e le potenziali minacce. Il loro lavoro consiste nell'identificare le vulnerabilità e presentare le raccomandazioni per risolvere tali problemi.
- Amministratore di sicurezza informatica: si occupa di gestire la sicurezza informatica delle organizzazioni. Svolge un ruolo fondamentale nel garantire che i sistemi informatici siano protetti e che le politiche di sicurezza informatica siano rispettate.

A PORTATA DI MANO

INQUADRA IL QR CODE O VAI AL LINK:

https://www.menti.com/alzoqw3wi3r1

LA PAROLA ALL'ESPERTO
Prof. Paolo Primetto

SFATIAMO QUALCHE FALSO MITO SUGLI HACKER

1. Gli hacker sono tutti criminali: Questo è uno dei falsi miti più comuni. Mentre alcuni hacker sono coinvolti in attività criminali, come l'hacking di sistemi informatici o il furto di dati personali, non tutti gli hacker sono criminali. Ci sono anche hacker etici, che lavorano per migliorare la sicurezza dei sistemi informatici.
2. Gli hacker sono tutti giovani: Questo falso mito deriva dal fatto che molti hacker famosi sono stati adolescenti quando hanno iniziato la loro attività. In realtà, gli hacker possono essere di qualsiasi età e di qualsiasi genere. L'età media degli hacker è in realtà piuttosto alta, e molti di loro hanno lavorato per anni nell'ambito dell'informatica.
3. Gli hacker sono tutti maschi: Anche se la maggior parte degli hacker sono uomini, ci sono molte donne che lavorano nel campo dell'hacking. Inoltre, ci sono molti gruppi di hacker che lavorano insieme, e questi gruppi possono includere persone di qualsiasi genere.
4. Gli hacker usano solo computer di ultima generazione: Questo falso mito deriva dal fatto che molte rappresentazioni cinematografiche mostrano gli hacker che usano computer potenti e costosi. In realtà, gli hacker possono utilizzare qualsiasi tipo di computer, anche quelli più economici.
5. Gli hacker sono tutti programmatori esperti: Questo falso mito deriva dal fatto che molte attività di hacking richiedono conoscenze avanzate di programmazione. Tuttavia, non tutti gli hacker sono programmatori esperti. Alcuni hacker utilizzano strumenti di hacking già esistenti, mentre altri si concentrano sulla ricerca di vulnerabilità nei sistemi informatici.

LO SAPEVI CHE ESISTONO MOLTE CATEGORIE DI HACKER?

1. Hacker white hat: anche conosciuti come «hacker etici» o «hacker di sicurezza». Questi lavorano per proteggere i sistemi informatici dalle vulnerabilità e dagli attacchi. Solitamente sono assunti dalle aziende per testare la sicurezza dei loro sistemi informatici e identificare eventuali falle.
2. Hacker black hat: anche conosciuti come «hacker malintenzionati» o «hacker cracker». Questi utilizzano le loro conoscenze per violare la sicurezza dei sistemi informatici a scopi illeciti, come il furto di dati personali, il danneggiamento dei sistemi o il furto di proprietà intellettuale.
3. Hacker grey hat: sono un'intermediazione tra le due tipologie precedenti. Questi possono violare la sicurezza dei sistemi informatici, ma lo fanno senza avere l'intenzione di causare danni. Spesso cercano di attirare l'attenzione sui problemi di sicurezza dei sistemi informatici, segnalando le falle che hanno trovato ai proprietari dei sistemi.
4. Hacker script kiddie: sono hacker inesperti che utilizzano strumenti di hacking preconfezionati e facili da usare, creati da hacker più esperti e permettono di condurre attacchi senza conoscere i dettagli tecnici dell'hacking.
5. Hacker hacktivist: utilizzano le loro conoscenze per promuovere una causa politica o sociale. Questi possono attaccare i siti web delle aziende che si oppongono alla loro causa o rubare e diffondere informazioni riservate per sensibilizzare l'opinione pubblica.
6. Hacker state-sponsored: sono hacker che agiscono su mandato di uno stato o di un governo. Questi possono essere impiegati per rubare informazioni sensibili o per condurre operazioni di spionaggio informatico.

UN ATTACCO INFORMATICO IN SINTESI

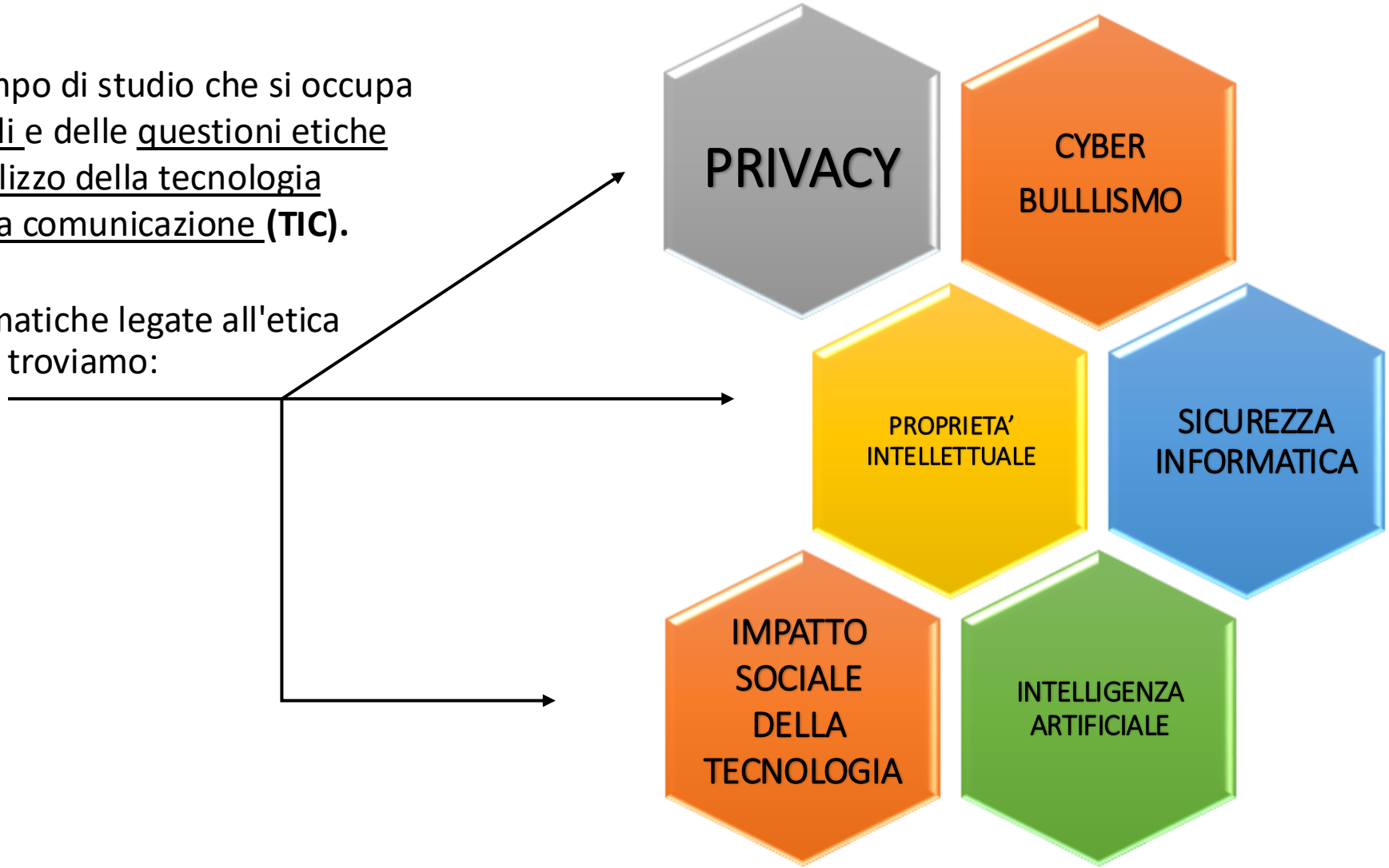
1. Raccolta di informazioni: durante questa fase, l'hacker cerca di raccogliere informazioni sulla potenziale vittima dell'attacco, come il tipo di sistema operativo in uso, i servizi di rete attivi, le vulnerabilità note e le password.
2. Scansione della rete: individuare le vulnerabilità del sistema, identificare le porte aperte e cercare di accedere ai servizi di rete vulnerabili.
3. Fase di ingresso: l'hacker cerca di infiltrarsi nel sistema, ad esempio attraverso la pubblicazione di exploit o di attacchi di phishing.
4. Escalation dei privilegi: l'hacker cerca di ottenere maggiori privilegi per accedere a dati riservati o per poter eseguire operazioni riservate. Ciò potrebbe avvenire attraverso l'uso di backdoor, exploit o tramite l'ingegneria sociale.
5. Mantenimento dell'accesso: l'hacker cerca di mantenere l'accesso al sistema, ad esempio installando software di controllo remoto o di malware.
6. Movimento laterale: l'hacker cerca di espandersi all'interno della rete, individuando altre potenziali vittime e sfruttando le vulnerabilità.
7. Azione finale: l'hacker compie l'azione per cui ha eseguito l'attacco, come il furto di dati, il sabotaggio del sistema o la richiesta di un riscatto.

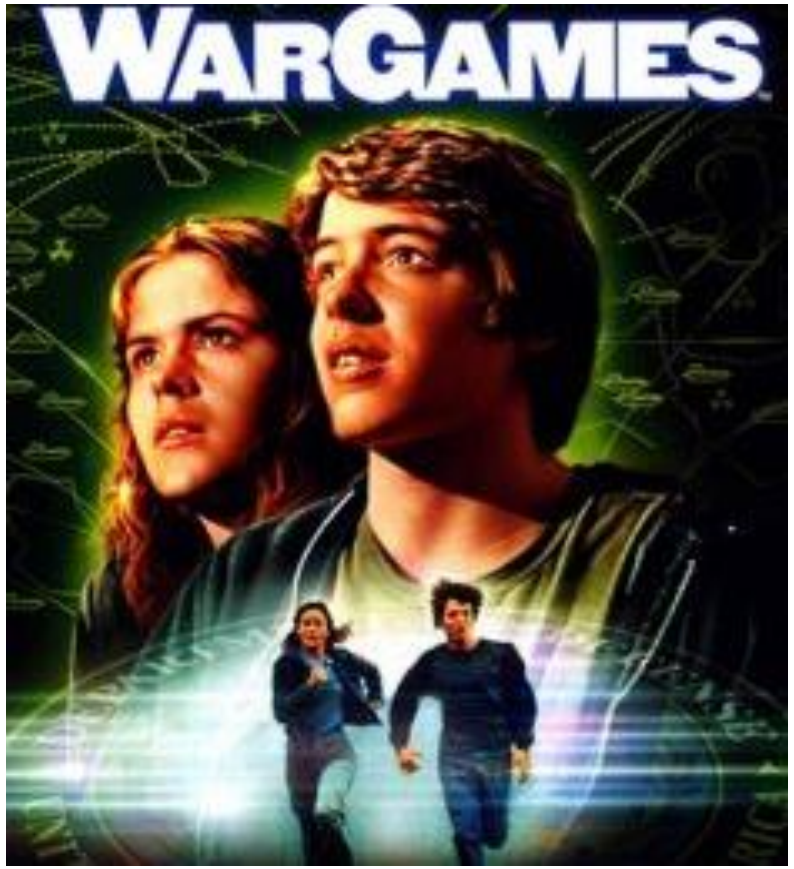
Le fasi di un attacco informatico possono variare a seconda dell'obiettivo dell'hacker e delle vulnerabilità del sistema bersaglio. Tuttavia, comprendere queste fasi può aiutare a proteggere i sistemi informatici dalle minacce e ad adottare misure preventive.

LO SAPEVI CHE ESISTE ANCHE L'ETICA INFORMATICA?

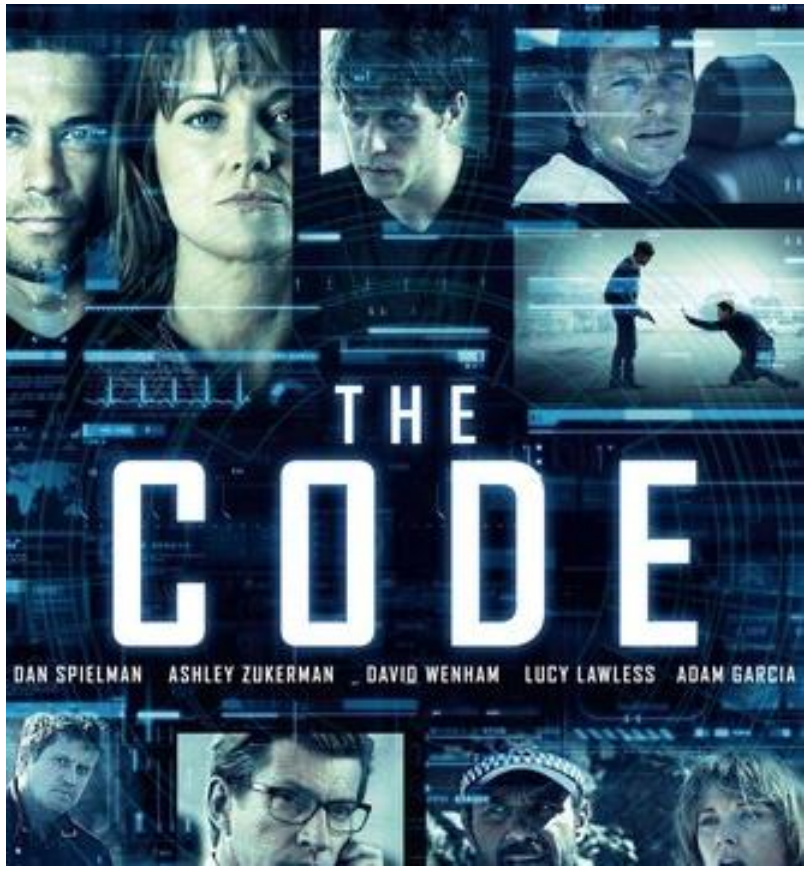
L'etica informatica è un campo di studio che si occupa dell'analisi dei valori morali e delle questioni etiche che emergono nell'utilizzo della tecnologia dell'informazione e della comunicazione **(TIC).**

Tra le principali problematiche legate all'etica informatica troviamo:





FILM CON HACKING REALISITICO



SERIE TV CON HACKING REALISITICO

FILMOGRAFIA E SERIE TV

FILMOGRAFIA

- *The Matrix* (Matrix), regia di Lana e Lilly Wachowski (1999)
- *Sneakers* (I Signori della Truffa), regia di Phil Alden Robinson (1992)
- *WarGames* (Giochi di guerra), regia di John Badham (1983)
- *The Social Network*, regia di David Fincher (2010)
- *Blackhat*, *regia di* Michael Mann (2015)

SERIE TV

- *Mr. Robot*, ideata da Amin Hammani (2015-2019)
- *Silicon Valley*, ideata da Mike Judge, John Altschuler, Dave Krinsky (2014-2019)
- *Black Mirror*, ideata da Charlie Brooker (2011-in produzione)
- *Halt and Catch Fire*, ideata da Christopher Cantwell, Christopher C. Rogers (2014-2017)
- *The Code*, ideata da Shelley Birse (2014-2016)

USCITE DI SICUREZZA

"I want to go to Venice to eat ice cream"

and abbreviating it to

"!w2g2V3n!c323!c"

123456

1-Ls7;O2+L_aU3*Wp-7g,I

1L MΩNDΩ
D3LL3 P455WΩRD
D1 S1CUR3ZZ4

FACCIAMO UN GIOCO…
«QUANTO E' SICURA LA TUA PASSWORD?»

PASSO 1: Vai sul sito **PASSWORD MONSTER** e scrivi una password SIMILE a quella che usi normalmente e scopri in quanto tempo riuscirebbero a craccarla!

https://www.passwordmonster.com/

PASSO 2: In 5 minuti, cercate di creare, singolarmente o in gruppi, una Password il più possibile efficace e sicura!

PASSO 3: Inserite nel sito le password da voi create e controllate chi ha ottenuto il miglior risultato!

3…2…1…VIA!

FACCIAMO UN GIOCO…
«QUANTO E' SICURA LA TUA PASSWORD?»

SCRIVETE QUI DI SEGUITO
LE PRIME TRE PASSWORD VINCITRICI:

1. …

2. …

3. …

FACCIAMO UN GIOCO...
«QUANTO E' SICURA LA TUA PASSWORD?»

SCRIVETE QUI DI SEGUITO
LE TRE PASSWORD PEGGIORI:

1. ...

2. ...

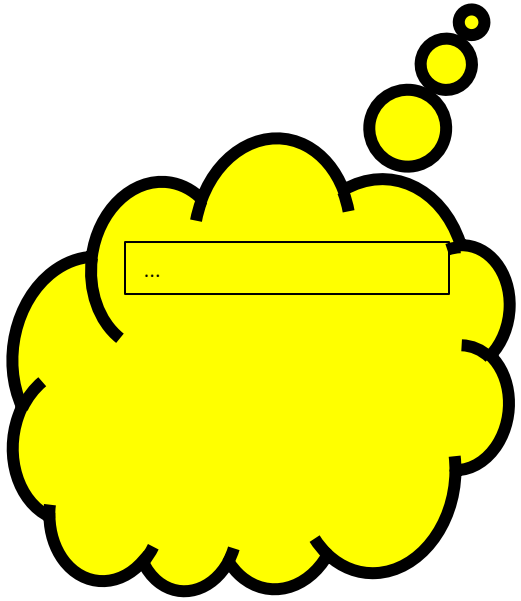
3. ...

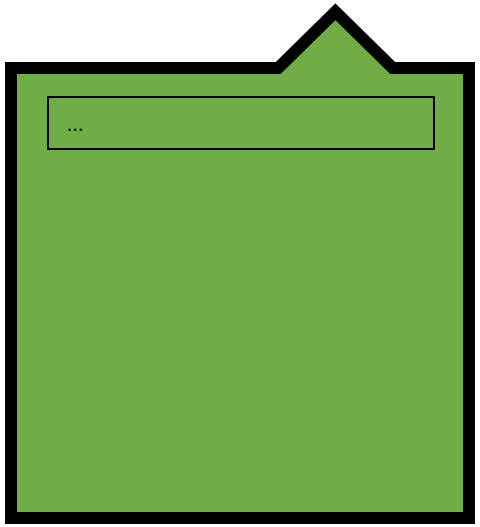
FACCIAMO UN GIOCO...
«QUANTO E' SICURA LA TUA PASSWORD?»

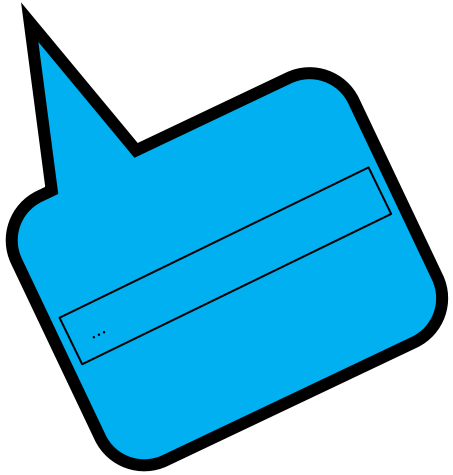
RAGIONIAMO INSIEME:

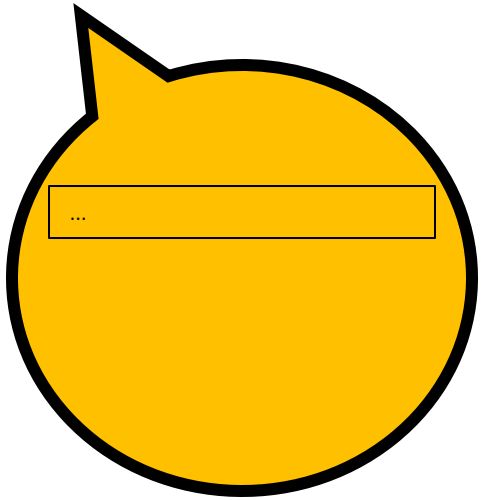
- PERCHE' ALCUNE PASSWORD SONO PIU' SICURE DI ALTRE?
- QUALI SONO LE CARATTERISTICHE CHE RENDONO UNA PASSWORD SICURA?

SCRIVETELO QUI DI SEGUITO









10 BUONE PRASSI DI SICUREZZA INFORMATICA

1. Cambiare le password predefinite: molte periferiche di rete vengono fornite con password predefinite. Queste sono facilmente scopribili e devono essere cambiate.
2. Aggiornare regolarmente i dispositivi: gli aggiornamenti includono spesso *patch* di sicurezza importanti. Bisogna assicurarsi che tutti i dispositivi siano aggiornati alla versione più recente del *software*.
3. Utilizzare una rete Wi-Fi sicura: utilizzare la crittografia WPA2 per proteggere la rete Wi-Fi. Evitare di utilizzare la crittografia WEP, che è facilmente violabile.
4. Disattivare la connessione automatica alle reti Wi-Fi pubbliche: queste reti sono spesso non sicure e possono esporre i dati a rischio di accesso non autorizzato.
5. Utilizzare software antivirus: per proteggere i dispositivi domestici da *virus* e *malware*.
6. Utilizzare la crittografia: per proteggere i dati sensibili e assicurarsi che le informazioni personali siano sempre criptate quando si inviano o si ricevono.
7. Evitare di condividere informazioni personali online: come numeri di telefono, indirizzi e-mail, informazioni finanziarie o informazioni di login sui social media e sui siti web non affidabili.
8. Fare attenzione alle e-mail di *phishing*: queste cercano di ingannare l'utente a fornire informazioni personali o a cliccare su un link dannoso.
9. Utilizzare un firewall: per proteggere la rete domestica da accessi non autorizzati.
10. Configurare correttamente le impostazioni di *privacy* sui dispositivi: per limitare l'accesso a informazioni personali e sensibili.

USCITE DI SICUREZZA

Per i contenuti si ringrazia:

Fabio C.

Silvio C.

Promosso e finanziato da:

Città di Torino

Progetto realizzato da:

ismel

orso

MAGAZZINI Oz

UTILE PER IL SOCIALE